Securing Billion Bluetooth Devices Leveraging Learning-Based Techniques

Hanlin Cai

National University of Ireland Maynooth, Maynooth, Co. Kildare, Ireland
Maynooth International Engineering College, Fuzhou University, Fujian, China
hanlin.cai.2021@mumail.ie

Abstract

As the most popular low-power communication protocol, cybersecurity research on Bluetooth Low Energy (BLE) has garnered significant attention. Due to BLE's inherent security limitations and firmware vulnerabilities, spoofing attacks can easily compromise BLE devices and tamper with privacy data. In this paper, we proposed *BLEGuard*, a hybrid detection mechanism combined cyber-physical features with learning-based techniques. We established a physical network testbed to conduct attack simulations and capture advertising packets. Four different network features were utilized to implement detection and classification algorithms. Preliminary results have verified the feasibility of our proposed methods.

Introduction

Bluetooth Low Energy is one of the most widely used protocols for Internet of Things devices (e.g., smart lights, smart sensors and smart thermostats). It is expected that the number of BLE devices will reach 7.5 billion by 2027. Unfortunately, these devices are vulnerable to spoofing attacks since most of them have limited I/O capabilities and do not support firmware updates. To address the security challenges, an out-of-the-box detection method has been proposed, leveraging BLE's cyber-physical features to defend against advanced spoofing attackers without requiring any interference or updates (Wu et al. 2020). Additionally, several works rely on learning-based techniques to identify the malicious packets within BLE networks. A learning framework that integrates supervised and unsupervised learning was suggested to classify packets as benign or malicious inside suspicious data batch with high precision (Lahmadi et al. 2020). However, most existing methods struggle to strike a balance between high accuracy, low false alarm rate and detection cost, which limits their applicability to a narrow range of scenarios. In this paper, we present *BLEGuard*, a hybrid detection mechanism based on cyber-physical features judgment and machine learning technology, which can identify advanced spoofing attacks through offline training and online analysis. Our contributions include: (i) physical BLE network testbed was built for attack simulations, (ii) detection mechanism was designed to recognize attacks efficiently, and (iii) experiments were conducted based on an imbalanced dataset.

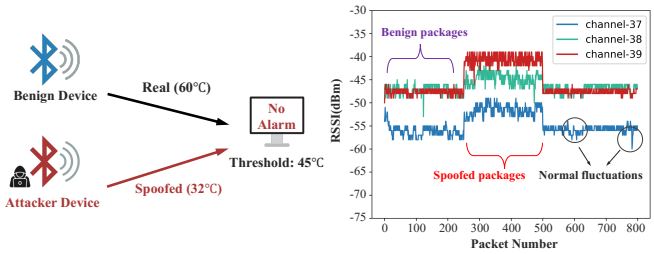

Figure 1: Left: Spoofing attack in BLE sensor network. Right: Observed RSSI values during attack simulation.

Experiment Setup

BLE Network Basics. The communication procedures between BLE devices and user devices can be categorized into four steps: advertising, connecting, pairing and accessing. However, most BLE network activities do not perform secure pairing and exchange data without conducting a secure authentication mechanism. This vulnerability can easily be exploited by attackers to inflict spoofing attacks. **Figure 1 (Left)** shows a typical spoofing attack case in BLE network.

Testbed Deployment. In this work, we built a physical BLE testbed in a typically noisy and complicated indoor office to evaluate our detection mechanism. We deployed sixteen popular BLE devices covering various Bluetooth chips to set up our testbed. Besides, three network sniffers were implemented based on the Raspberry Pi equipped with Ubertooth One, an open platform for capturing advertising packet.

Feature Selection. Considering the specificity of BLE networks, four representative cyber-physical features were used for detection algorithm design and learning models training:

- Used Channel Numbers (*UCN*): the data channels number used during the communication of the BLE packets.
- Advertising Interval (*INT*): the time gap between two continuous packets on the same advertising channel.
- Received Signal Strength Indicator (*RSSI*): the signal-to-noise ratio value available in BLE packets exchange.
- Carrier Frequency Offset (*CFO*): the unique offset between the designated and the actual carrier frequencies.

Attack Simulations. To generate multiple spoofing attacks, we utilized four distinct types of attacker platforms, each

with three identical samples at different locations. In the spoofing attack scenario, the cyber-physical features of BLE network will undergo noticeable affected, resulting in significant deviations from the benign scenario. For instance, the anomalous shift in the *RSSI* values of the advertising packets indicates the presence of spoofing attacks, as shown in **Figure 1 (Right)**. Currently, we have amassed a dataset comprising 1,010,526 advertising packets, with benign packets accounting for 85.2% and malicious packets for 14.8%.

Detection Mechanism

Pre-detection Algorithm. The specificity features of advertising packets can be used to determine malicious activities within BLE networks. The abrupt changes in *UCN* and *INT* can be attributed to the occurrence of potential attacks. Additionally, to detect the advanced spoofing attacks, *RSSI* and *CFO* are utilized to implement a continuous pre-detection mechanism. In BLEGuard, three network sniffers are utilized to collect the value of *RSSI* and *CFO* in the lookback window to infer valid ranges, and then inspect relevant values of advertising packets in the observation window. Once the system detects an abnormality in either of these features, an alarm will be raised. This pre-detection algorithm can be easily deployed in BLE network without any interference.

Reconstruction Model. The reconstruction model involves learning the benign behavior of BLE packet exchanges. In the offline training phase, we aim to minimize the error between learned data D_L and original dataset D_T. In the online testing phase, if input data contains any malicious packet, the reconstruction error will obviously increase. The network reconstructions are conducted using a temporal convolutional network (TCN). The residual is defined as $R(D_T, D_L) = |D_T - D_L|$ with $D_L = f(D_T)$ and f represents the transformation of TCN auto-encoder. Afterwards, we evaluate the residual to determine the anomaly score α for each data batch, as illustrated in Equation (1), where R_α represents the corresponding residual, μ is the mean value of residual, and σ is its standard deviation. In a word, reconstruction methods are employed to detect suspicious data batches, in next step, we will utilize the classification model to identify the malicious packets in each suspicious batch.

$$\alpha = \begin{cases} 0, \ when \ |R_\alpha - \mu R_\alpha| \leq 3 * \sigma R_\alpha \\ 1, \ when \ |R_\alpha - \mu R_\alpha| > 3 * \sigma R_\alpha \end{cases} \quad (1)$$

Classification Models. Upon the identification of suspicious batches, the next stage is to categorize these packets into different classes: benign or malicious. In this work, the text-convolutional neural network (text-CNN) (Chen et al. 2022) is employed for traffic feature extraction, while the packet classification will be conducted using four cost-efficient classifiers (SVM, KNN, Random Forest and Naïve Bayes) to prevent bias in text analysis. The network payload-based features are generated by converting the payload bytes into low dimensional vectors utilizing the *Word2Vec* techniques. These vectors served as the input for the text-CNN, and the extracted key features were concatenated with statistical features and provided for the final classification models.

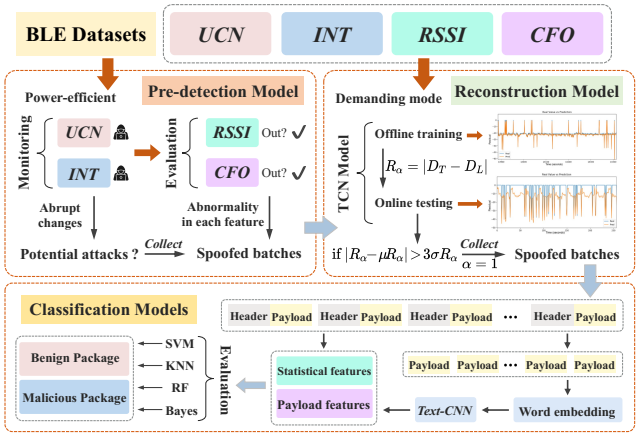

Figure 2: The workflow of BLEGuard detection mechanism.

Hybrid Detection Mechanism. Overall, BLEGuard system aims to balance the detection accuracy and power overhead within BLE networks. As shown in **Figure 2**, when GPU resources are limited, pre-detection algorithm can be effectively deployed with very low online consumption, while reconstruction models can be activated when the detection accuracy is paramount. In addition, the classification models can identify specific malicious advertising packets reliably and provide fine-tune feedback to the detection modules. We provided our code for the reproducibility of experiments[1].

Results and Discussion

The experiments utilized a large-scale, imbalanced dataset to evaluate the performance of BLEGuard system. The results revealed a high level of effectiveness, achieving an average accuracy of 98.01%, with a false alarm rate of 0.09% and an undetection rate of 1.28%. The future work aims to expand experiments into some known real-world spoofing attacks.

Acknowledgements

This project was supported by the Chinese National Undergraduate Innovation Training Program (No. 202310386056). Thank you to Dr. Tozammel Hossain and Dr. Zhezhuang Xu.

References

Chen, X.; Hao, Z.; Li, L.; Cui, L.; Zhu, Y.; Ding, Z.; and Liu, Y. 2022. Cruparamer: Learning on parameter-augmented api sequences for malware detection. *IEEE Transactions on Information Forensics and Security*, 17: 788–803.

Lahmadi, A.; Duque, A.; Heraief, N.; and Francq, J. 2020. MitM attack detection in BLE networks using reconstruction and classification machine learning techniques. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, 149–164. Springer.

Wu, J.; Nan, Y.; Kumar, V.; Payer, M.; and Xu, D. 2020. {BlueShield}: Detecting spoofing attacks in bluetooth low energy networks. In *23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)*.

[1]Link: https://github.com/BLEGuard/supplement